

Canaudit Perspective

February 2004
Volume 5, Issue 2

Topics of Interest:

- Executive Management Relies on the SOX Audit
- How Can I Determine if the SOX Test is Compromised?
- We Have Too Many Issues to Correct, What Do We Do?



Sarbanes Oxley: Compliance or Sham?

Written by: Gordon Smith
President, CEO
Canaudit, Inc.

Much has been written about Sarbanes-Oxley (SOX) in the last few months. In this article, I am going to take a contrarian's approach. I am very concerned that some organizations may be seeking ways to appear to be in compliance to SOX, from an information technology standpoint, when, in reality, they are not. The legislation is very clear. IT controls are required and significant IT control issues must be disclosed. I am in complete agreement with this disclosure requirement as I believe it will result in stronger controls and a more secure business environment.

For years, IT auditors and security managers identified significant control weaknesses; yet, management chose not to address them. With SOX in place, significant issues not only are being identified, but they are being resolved! From a public relations standpoint, it is far better to protect the data properly than it is to admit that there are serious control issues in the SOX disclosures.

I am very concerned that some organizations may not be forthright in their SOX reporting. We recently received a proposal to conduct a SOX security test. The test would be limited to specific machines that contain financial information. There were very specific rules of engagement. We could only test the prespecified machines. We were not permitted to attempt to escalate access to the administrator or root level if we gained user access. Also, if we found a way to gain direct administrator-type access using an exploit or default passwords, we were not permitted to perform the test. Any issues we identified would be disclosed at the completion of the preliminary audit. We would return after the IT folks had time to correct the issues. Only items that were not corrected would be included in our audit report.

This proposed testing had several flaws. The prohibition against gaining administrative rights prevents the audit team from assessing the security on the machines. Without these rights, we cannot test the security settings, which can include the account, audit and password policies. In the UNIX environment, we cannot determine if root-protected trust relationships exist, which could compromise security, or if there are other weaknesses that could enable financial data to be altered or worse – deleted. Administrative rights are necessary to gain the encrypted passwords in the Windows environment and the shadow password file in the UNIX environment. Password strength cannot be tested unless the audit team has access to the required files.

These test restrictions turned the audit into a sham in my humble opinion. Limiting tests solely to the machines that contain SOX-related data does not enable the audit team to test for network-wide vulnerabilities that have a negative impact on SOX-related machines and application data. For instance, if the team could gain administrative access on a poorly secured Windows machine, we could download and crack the password file. Using these compromised accounts and passwords, we may be able to access the machines containing SOX-

related data. If executives are going to sign off on the internal control structure, then they should have the knowledge they need to do so. This information should not be skewed or altered in any way. Only a complete and unrestricted test can provide the assurance they need to comply with the legislation. We chose not to bid on the job given the constraints placed upon the audit team by the potential client. Independence is an essential component of our audit philosophy. Without it, we cannot and will not perform an audit or security review.

The question that now must be resolved is why would the client want to skew the test? Well, the answer is in section 302 of the SOX legislation. This section requires that the CEO and CFO certify the financial statements and disclosures are fairly presented. A violation occurs if the CFO or CEO knowingly and intentionally certifies statements that they should not certify. If the audit does not identify any serious issues, then the CFO and CEO will not know of any reportable internal control issues. They can sign the statements in good faith. Since they would not know that the test was skewed, they really did nothing wrong. At least, that will be the spin released by the public relations person after a serious SOX violation is discovered. I believe that limiting testing to ensure that serious issues cannot be discovered may not be illegal, but violates the spirit of SOX.

Executive Management Relies on the SOX Audit

Your executives want assurance that all financial data is properly protected. They are the ones signing on the bottom line and it is their bonuses that are at risk should there be a restatement. I believe that it is important to ensure that SOX testing is both thorough and independent. The executives want to know if there are serious issues, and more importantly, they will want any issues corrected or mitigated prior to the issuance of the financial statements and the required certifications.

Unfortunately, there may be political reasons for others to want to influence the testing. If executive management has been assured that the required controls are in place, they will be surprised to find serious control issues. They will question those who gave them false assurances. It is highly likely that they will want the person who misled them terminated immediately. Some managers believe that there will never be a problem at their organization. Therefore, they are willing to take the risk for their own personal and political gain. These individuals will issue instructions to control the test, thereby ensuring that no serious issues are discovered. The cover-up will be sustained until a serious computer incident occurs and is reported on the front page of the Wall Street Journal.

How Can I Determine if the SOX Test is Compromised?

The first place I look is in the disclosure section of the audit report. Any restrictions placed on the audit will normally be stated here. You should also check the original request for proposal that was sent to potential bidders. Normally, the project scope and any constraints will be documented in the RFP (Request for Proposal). Often vendors are asked to submit any questions they have in writing. You should check the questions and the answers to determine if any audit limitations are detailed in the answers to the questions.

The testing performed will be explained if the report was prepared by a reputable firm. Testing should encompass full operating system and network tests of the machines containing SOX-related data. Identifying controls through the interview process is convenient, but does not confirm that the control is actually in place. Each machine required to be protected for SOX purposes must be tested to ensure that it is properly hardened and that all required controls are in place.

We Have Too Many Issues to Correct, What Do We Do?

There could be some major issues in your network that cannot be fixed before the statements must be issued. In that case, there are several solutions. The first is to thoroughly test the machines to identify those with significant control issues. Missing required patches and poor password control are the most common issues. Other items such as legacy software issues are more complex and may not be correctable in the short term. Once the testing is complete, identify those items that have a high SOX impact, yet are inexpensive to correct. These should be corrected right away. Items which have a high SOX impact and are expensive to correct may be handled

differently. For instance, if a legacy software application would need to be replaced at \$50,000,000 and would take several years to complete, obviously it cannot be corrected prior to releasing the SOX reporting.

We suggest that other controls be used to protect the machines which cannot otherwise be protected prior to the issuance of the SOX report. One technique we recommend is to place these machines into one or two network subnets. They can be physically located in any secure facility; however, logically they are clustered into one subnet. Once these machines are clustered in the required subnets, they can be protected with a firewall, switch or router using access control lists (ACLs). These lists limit access to those who need access to the machines to perform their business functions. Clustering users into groups facilitates this process. The example I used above enables the installation of a strong control to prevent unauthorized access.

A secondary control is also required. Since we know that the operating system or application is soft from a control standpoint, we can add in a honeypot to detect when the network segment containing SOX-related machines is under attack. We suggest the use of Back Officer Friendly, a free shareware product, for this purpose. You can download a copy of this tool from the Canaudit website. By using these two simple techniques you will have protected the poorly controlled machines and will know if someone is trying to attack them. When an attack is detected, intrusion incident mitigation and investigation procedures should be invoked.

There are many ways to protect SOX machines. The above example was just one method of dealing with machines that cannot readily be secured. There are other techniques that can also be used to improve control, while seeking a better and more permanent solution. It is better to install a control to mitigate the issue, rather than limit SOX testing. Corporate executives and the Board need to know the true extent of internal control and the weaknesses. This will enable them to fully understand the need for enhanced controls and the funding required to properly protect financial information. They will fund longer term remediation projects provided they understand the full extent of the security issues.

In closing, I want to emphasize that the “don’t test / don’t know” philosophy will eventually backfire. One day, there will be a computer incident. When it does, the executives are going to have egg on their face for signing the SOX disclosure. They may even have to pay back their bonuses. At that point you can be sure they will be looking for those who deceived them into believing that controls were “adequate.” I believe that it would be far better to tell the executives and Board now that: there are issues, that we have a short-term mitigation plan, and that we are seeking funding for a mid- and long-term remediation plan. Not only is it truthful, but it is sound business practice.

As always, the opinions expressed in this short article are mine and mine alone. I do look forward to receiving your comments, both positive and negative. Send your comments to Gordon@canaudit.com



Gordon Smith
President, CEO

1376 Erringer Road, Simi Valley, CA, 93065
Telephone: (805) 583-3723 – Fax: (805) 582-2676 – Web site: www.canaudit.com